Mr. Chairman,

I have the honour to make the following general statement with regard to draft resolution A/C.1/69/L.26 entitled “Developments in the field of information and telecommunications in the context of international security”. This statement is made on behalf of Australia, Austria, Belgium, Bulgaria, Canada, Chile, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Mexico, Montenegro, the Netherlands, New Zealand, Nigeria, Norway, Poland, Portugal, the Republic of Korea, Romania, Slovakia, Slovenia, Switzerland, Tunisia, Turkey, the United Kingdom, the United States, Uruguay and my own country, Sweden.

We join the consensus on draft resolution L.26. We would however like to stress some relevant aspects in this context.

International deliberations on cyberspace issues and the use of ICTs in an international security context need to continue to evolve as we seek greater common understanding and shared views of these issues globally. One noteworthy development in this regard was the adoption on 24 June 2013 of a report by the third UN Group of Governmental Experts (UN GGE) on “Developments in the Field of Information and Telecommunications in the Context of International Security”.

The 2012-13 UN GGE made a significant contribution towards building an effective framework for international norms of responsible behaviour by states on the basis of existing international law and practical cooperative measures. We welcome these efforts and the adoption by consensus of the report. We also encourage the new UN GGE – which held its first session this past July - to build and advance this important work while fully taking some crucial principles and concepts into account.

One fundamental point for our delegations regarding the key features of the internet is that it should remain open, thereby facilitating a free flow of information in cyberspace. For us, one principle is very basic: The same rights that individuals have offline must also be protected online, in particular freedom of expression, including the freedom to seek and impart information, and freedom of assembly and association. Hence, we welcome resolution 20/8 at the 20th session of the UN Human Rights Council in 2012, which affirms this basic understanding. We note that the resolution was adopted by consensus, giving it a very broad cross-regional backing. A follow-up resolution (26/13) was adopted in the Human Rights Council without a vote on 20 June this year, reaffirming the main messages from the 2012 resolution while including important additions on the importance of internet access for global development and the right to education.

While we would prefer a direct reference to HRC resolution 20/8, we note the reference – introduced last year - in draft resolution L.26 to the importance of respect for human rights in the use of ICTs as an important step in the right direction.

Mr. Chairman,

An open, free and secure Internet used for peaceful purposes is essential for economic, social and political development in the 21st century. The Internet has developed successfully without government control. The bottom-up, innovation-driven approach to building the Internet has been key to its success, and mirrors the distributed character of the underlying technology. Another fundamental position for our
delegations is therefore that discussions with wider implications for the future of the Internet should be based on a multi-stakeholder approach that includes private sector and civil society actors.

Our societies’ increasing dependence on information technology has brought with it new challenges. Security in an increasingly interconnected world will, to a great extent, revolve around protecting information flows and the integrity of critical ICT infrastructures. Cyber-attacks, cyber espionage and cybercrime, as well as lack of public awareness of the everyday aspects of cybersecurity, are realities in today’s cyber domain and these risks and vulnerabilities need to be addressed. This also implies challenges, as our traditional tools of addressing these risks have yet to adapt to the global and boundless nature of cyberspace.

It is clear, however, that the work against threats to our freedom and security in cyberspace can only be tackled effectively through global cooperation between states as well as the private sector and civil society. In this regard we welcome the reference made to the role of the private sector and civil society in the GGE report and emphasize the crucial importance of taking all relevant stakeholders into account on an equal and appropriate footing while advancing this important work. We also welcome the reference made to the importance of capacity building to an effective global effort on securing ICTs and their use. We support the proposed measures and will welcome further international commitment to such work.

Mr. Chairman,
In addressing cyber challenges we must continue to engage in an international discussion on norms and principles of responsible state behaviour consistent with the affirmation by the recent GGE report that international law is applicable in guiding State activities in cyberspace, while underscoring as well the key role to be played by confidence-building and transparency measures.

In this regard, we strongly support the affirmation made by the 2012-13 GGE that the application of norms relevant to the use of ICTs by States is an essential measure to reduce risks to international peace, security and stability. We also welcome the recommendation by the GGE on the need of further study on common understandings on how such norms shall apply to State behaviour and the use of ICTs by States.

The 2013 GGE report underlines that voluntary confidence building measures can promote trust and assurance among States and help reduce the risk of conflict by increasing predictability and reducing misperception. Such measures can make an important contribution to addressing the concerns of States over the use of ICTs by States and could be a significant step towards promoting international security. We support these recommendations and encourage further work along those lines, including in regional security and confidence building frameworks.

We engage in these discussions on the basis that existing international law is applicable and that our universal values of human rights, democracy and the rule of law guide our deliberations on norms in cyberspace.

We call for these crucial aspects to guide further work in the cyber area, including in the context of addressing international security aspects of the use of ICTs in the format of the UN GGE.

Thank you.